

**UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION**

AMABEL LIN, individually and on behalf of
herself and all others similarly situated,

Plaintiff,

v.

LENDING TREE, LLC;

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Amabel Lin (“Plaintiff”), on behalf of herself and all others similarly situated, alleges the following Class Action Complaint (the “Action”) against the above-captioned Defendant Lending Tree, LLC (“Defendant” or “LendingTree”) upon personal knowledge as to herself and her own actions, and upon information and belief, including the investigation of counsel as follows:

I. NATURE OF THE ACTION

1. This Action arises out of the 2022 data breach (the “Data Breach”) involving Defendant, Lending Tree, LLC, a publicly-traded online marketplace for loan services.

2. LendingTree failed to reasonably secure, monitor, and maintain private and sensitive personal information provided by consumers and potential consumers (collectively referred to hereinafter as “consumers”) including, and without limitation: full names, Social Security numbers, dates of birth, and street addresses (collectively, “PII”). This PII was stored on Defendant’s private network and was compromised by way of a “code vulnerability” that allowed an unauthorized third party to access the PII of Plaintiff and Class Members’ PII. As a result, Plaintiff and other consumers suffered present injury and damages in the form of identity theft, loss of value of their PII, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

3. Moreover, Plaintiff’s and Class members’ PII has already been released in unencrypted form and is available to download for free.¹

4. After learning of the Data Breach, Defendant waited nearly one month to notify Plaintiff and Class Members of the Data Breach and/or inform them that their PII was

¹ <https://restoreprivacy.com/lendingtree-data-breach-2022/>

compromised. Moreover, as shown in the Notice of Data Breach provided to Plaintiff and Class members, Defendant: (1) did not know or does not disclose to consumers the exact dates of the unauthorized disclosure (stating that it might have occurred in mid-February 2022); and (2) failed to adequately monitor their servers for unauthorized actors or disclosures, as they did not discover the unauthorized access of consumers' PII until almost four months after it is believed to have initially begun. All the while, from mid-February 2022 through at least June 3, 2022, Plaintiff and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

5. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant's conduct in breaching these duties amounts to negligence and/or recklessness and violates federal and state statutes.

6. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to take reasonable steps to protect the PII of Plaintiff and Class Members and warn Plaintiff and Class Members of Defendant's inadequate information security practices. Defendant disregarded the rights of Plaintiff and Class Members by knowingly failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use.

7. As a direct and proximate result of Defendant's data security failures and the Data Breach, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party, and Plaintiff and Class Members have suffered actual, present, and concrete injuries. These injuries include: (i) the current and imminent risk of fraud and identity theft (ii) lost or diminished value of PII ; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII; (vi) the invasion of privacy; (vii) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and the Class Members' PII; and (viii) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII.

8. Consumers' PII exposed by the Data Breach has been sold or is being offered for sale on the dark web, which is the *modus operandi* of cybercriminals.

9. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security.

10. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to damages, injunctive and other equitable relief to remedy the harm that resulted from Defendant's inadequate security practices.

II. JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of \$5,000,000.00 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members are citizens of a different state than Defendant; additionally, Plaintiff Lin is a resident of the state of Hawaii and Defendant maintains its principal place of business in North Carolina. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

12. This Court has personal jurisdiction over Defendant because it is headquartered in and maintains its principal place of business in this District.

13. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Defendant’s headquarters and principal place of business are located in this District, Defendant resides in this District, and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District, including, without limitation, decisions made by Defendant’s governance and management personnel or inaction by those individuals that led to misrepresentations, invasions of privacy, and the Data Breach.

III. PARTIES

Plaintiff Amabel Lin

14. Plaintiff Lin is, and at all relevant times has been, a resident of the state of Hawaii.

15. Plaintiff received a copy of the “Notice of Data Breach” letter dated June 29, 2022 from the Defendant. The letter informed Plaintiff that, on June 3, 2022, Defendant “determined that a code vulnerability likely resulted in the unauthorized disclosure of ... sensitive personal

information.” According to Defendant, “the unauthorized disclosure began in mid-February 2022.”

16. The type of data at issue included full names, Social Security numbers, dates of birth, and addresses which belonged to prospective and actual consumers of LendingTree’s loan aggregation services. The letter further advised Plaintiff that they should spend time reviewing credit reports, activate the insufficient credit monitoring and identity protection services offered by Defendant, and place fraud alerts with the three credit bureaus (Experian, Equifax, and TransUnion).

17. Defendant obtained and continues to maintain Plaintiff’s and Class Members’ PII and has a continuing legal duty and obligation to protect that sensitive information from unauthorized access and disclosure. Defendant required that Plaintiff entrust her PII to it on the understanding that her PII would be safeguarded from unauthorized access. Plaintiff, however, would not have entrusted her PII to Defendant had she known that it would fail to maintain adequate data security. Plaintiff’s PII was compromised and disclosed as a result of the Data Breach and Defendant’s failure to implement reasonable cyber security practices.

Defendant Lending Tree, LLC

18. Defendant Lending Tree, LLC is a Delaware limited liability company with its principal place of business located in Charlotte, North Carolina.

19. All of Plaintiff’s claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents, and/or assigns.

IV. FACTUAL ALLEGATIONS

Defendant's Business

20. LendingTree is “an online loan marketplace for various financial borrowing needs including auto loans, small business loans, personal loans, credit cards and more. [LendingTree] also offer[s] comparison shopping services for autos and educational programs. Together, these services serve as an ally for consumers who are looking to comparison shop among multiple businesses and professionals[.]”²

21. Plaintiff and Class Members, who are consumers, utilized LendingTree’s aforementioned services for their personal and household “financial borrowing needs.” Defendant required that consumers, including Plaintiff and Class members provide their PII as a condition of receiving services, and Plaintiff and Class members did in fact provide their PII to Defendant in conjunction with these services. Plaintiff’s and Class Members’ PII was required in order to fill out various forms in order to use said services, including loan applications, loan screenings, and other form documents associated with financial services of vendors that use LendingTree’s online marketplace.

22. Plaintiff and Class Members relied on the sophistication of Defendant and its network to keep their PII confidential and securely maintained, to use this information for consumer purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members reasonable expected and demand security to safeguard their PII.

23. Defendant required the submission of and voluntarily accepted the PII as part of its business and had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class

² <https://www.lendingtree.com/press/>, (last accessed July 31, 2022).

Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's PII safe and confidential.

24. The information held by Defendant in its computer systems and networks included the PII of Plaintiff and Class Members.

25. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Defendant requires that consumers provide their PII to it as a condition of using Defendant's online marketplace for financial services. Without the required submission of PII, Defendant cannot link loan providers to consumers and the marketplace itself would be unable to match lenders and borrowers.

26. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

27. Moreover, as a sophisticated financial entity, Defendant knew or should have known of the importance of safeguarding PII and the severe and long-lasting consequences that result when a consumer's PII is compromised.

28. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and expected that Defendant would do the same.

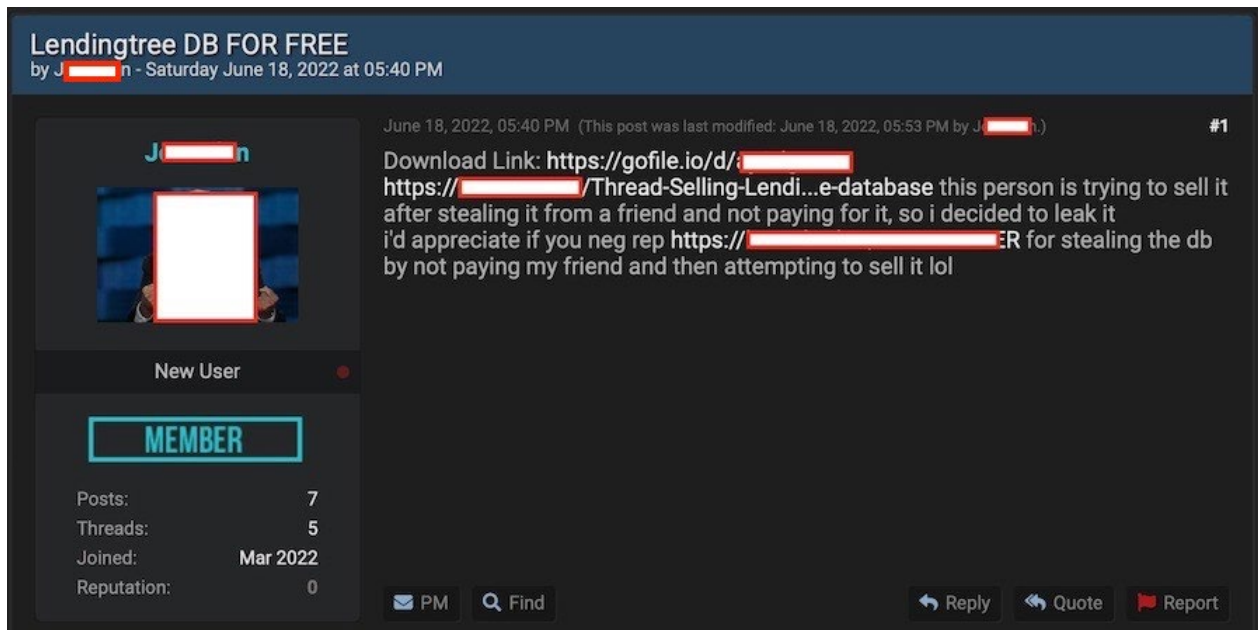
The Data Breach

29. At some point in mid-February 2022, an "unauthorized disclosure" of consumer PII entrusted to Defendant began due to an exploited code vulnerability within Defendant's computer network.³ This exploited code vulnerability was not discovered by LendingTree until June 3, 2022 – nearly four months after it began.⁴

³ Notice.

⁴ *Id.*

30. Shortly after Defendant discovered the Data Breach and before it noticed consumers, an unknown person posted a sample of the stolen PII and offered the full dataset for sale on a web forum.⁵ However, on June 18, 2022 another forum poster posted the entire dataset, apparently in response to a dispute with the original poster, containing the PII of 200,643 consumers.



31. After analyzing the dataset, Restore Privacy, a consumer advocacy group, identified additional information that was compromised by the Data Breach and which Defendant has not disclosed to affected consumers. Restore Privacy found that each of the 200,643 line items in the data set represented a unique consumer and each entry contained the following PII: email address; full name; physical address; phone number; IP address; loan type; home description, credit profile score; property use; and military status. Restore Privacy further confirmed that the dataset was exfiltrated from Defendant's network, even though Defendant has not yet detailed the full scope of the Data Breach to Plaintiff and Class members.⁶

⁵ <https://restoreprivacy.com/lendingtree-data-breach-2022/>

⁶ *Id.*

```

200635 f.[REDACTED]@yahoo.com,Michelle,[REDACTED],6[REDACTED]4, Fort
worth, TX, 76133, [REDACTED], 9[REDACTED]7, 11/2/2021
21:14, https://www.lendingtree.com/, Loan, Home Equity, Single
Family, Good(620-719), Primary Residence, no, "332,628"
200636 f.[REDACTED]@comcast.net, Susanna, [REDACTED], [REDACTED]
[REDACTED], Tucson, AZ, 85739, [REDACTED], 1[REDACTED], 11/2/2021
21:48, https://www.lendingtree.com/, Loan, Reverse Mortgage, Manufactured
Home, Lower, Investment Property, no, "112,742"
200637 [REDACTED]@gmail.com, Frances, [REDACTED], [REDACTED]
[REDACTED], Katonah, NY, 10536, [REDACTED], 2[REDACTED], 11/2/2021
15:42, https://www.lendingtree.com/, Loan, Reverse Mortgage, Multi
Family, Excellent(720), Secondary Home, yes, "177,079"

```

32. Defendant however, has only reported to Plaintiff and Class Members that the information compromised in the Data breach included names, Social Security numbers, dates of birth, and street addresses.⁷

33. After learning of the Data Breach, Defendant waited nearly one month to notify Plaintiff and Class Members of the Data Breach and/or inform them that their PII was compromised. Moreover, pursuant to the Notice of Data Breach, Defendant: (1) did not know or does not disclose to consumers the exact dates of the unauthorized disclosure (stating that it might have occurred in mid-February 2022) and (2) failed to adequately monitor their servers for unauthorized actors or disclosures, as they did not discover the unauthorized disclosure until almost four months after it is believed to have begun. Additionally, Defendant has apparently not disclosed the full scope of the compromised information even though a third party was able to analyze the stolen data set and identify that further private information was compromised. All the while, from mid-February 2022 through at least June 3, 2022, Plaintiff and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

⁷ Notice.

34. On or around June 29, 2022, LendingTree disseminated data breach notifications to consumers affected by the Data Breach dated June 29, 2022.⁸

35. On or around July 11, 2022, LendingTree disclosed the Data Breach to the California Attorney General's Office.⁹

36. Plaintiff's PII, and that of Class Members, was subsequently offered for sale on the dark web following the Data Breach, and then freely distributed on a web forum frequented by identity thieves and it is only a matter of time until that information is misused if it has not been already.

37. This is not the only cyber security incident experienced by Defendant. In 2008, Defendant publicly disclosed that it had suffered a data breach in which consumers' Social Security numbers, income, and employment data were accessed by unauthorized third parties.¹⁰ And, on January 6, 2022, Defendant also reported to the Indiana Attorney General's Office that it suffered from a data breach.¹¹ Accordingly, Defendant was on notice that it was a prime target for data thieves and that its methods of preventing and detecting cyber-attacks was insufficient. Nevertheless, Defendant did not detect the Data Breach until February of 2022, well after cyber thieves had exfiltrated Plaintiff's and Class Members' PII.

38. To prevent and detect cyber-attacks attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

⁸ *Id.*

⁹ <https://oag.ca.gov/ecrime/databreach/reports/sb24-555114>, (last accessed Jul. 31, 2022).

¹⁰ <https://www.reuters.com/article/iac-lendingtree-theft/lendingtree-reports-data-breach-idUSN286771320080428>

¹¹ <https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/JulyYear-to-date-Report.pdf>

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

39. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- Update and patch your computer. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- Use caution with links and when entering website addresses. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....
- Open email attachments with caution. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- Keep your personal information safe. Check a website's security to ensure the information you submit is encrypted before you provide it....
- Verify email senders. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- Inform yourself. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- Use and maintain preventative software programs. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....¹²

¹² See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at*: <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited Nov. 11, 2021).

40. To prevent and detect cyber-attacks attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹³

¹³ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at*: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Nov. 11, 2021).

41. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above standard measures to prevent and detect cyber-attacks.

42. The occurrence of the Data Breach and Defendant's failure to timely detect it indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyber attacks, resulting in the Data Breach and the exposure of the PII of at least 200,634 consumers, including Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members

43. Defendant has historically acquired, collected, and stored the PII of Plaintiff and Class Members.

44. As part of being a consumer of Defendant's online loan marketplace, Plaintiff and the Class Members are required to give their sensitive and confidential PII to Defendant. Defendant retains and stores this information and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to connect consumers and lenders on its online loan marketplace, as loan vendors require that PII to make loan decisions and offerings.

45. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

46. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

47. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members.

48. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts it received directed to protecting and securing sensitive data.

49. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

The Value of Personally Identifiable Information

50. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."¹⁴ The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."¹⁵

51. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.¹⁶ Experian reports that a stolen credit or debit card number can

¹⁴ 17 C.F.R. § 248.201 (2013).

¹⁵ *Id.*

¹⁶ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Jan. 19, 2022).

sell for \$5 to \$110 on the dark web.¹⁷ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁸

52. Social Security numbers, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.¹⁹

53. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

54. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link

¹⁷ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Jan 19, 2022).

¹⁸ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Jan. 19, 2022).

¹⁹ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Jan. 19, 2022).

the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”²⁰

55. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The PII compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change and Plaintiff and Class members will remain at risk of their PII being misused for years to come.

56. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”²¹

57. Among other forms of fraud, identity thieves may use Social Security numbers to obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

58. The fraudulent activity resulting from the Data Breach may not come to light for years.

59. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen

²⁰ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Jan. 19, 2022).

²¹ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Nov. 11, 2021).

data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²²

60. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

61. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

62. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

63. In the breach notification letter, Defendant made an offer of 24 months of credit and identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII or for the time and expense they will expend in response to the Data Breach.

²² *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Jan. 19, 2022).

64. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

65. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Defendant Violated the Gramm-Leach-Bliley Act

66. Defendant runs an online loan marketplace for consumers that provides or arranges financing or leasing options and is therefore subject to the Gramm-Leach-Bliley Act ("GLBA").

67. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendant was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1 et seq., and is subject to numerous rules and regulations promulgated on the GLBA Statutes. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the Consumer Financial Protection Bureau ("CFPB") became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

68. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

69. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and

conspicuous.”¹⁶ C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. “Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.” 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must “accurately reflect[] [the financial institution’s] privacy policies and practices.” 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution’s security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided “so that each consumer can reasonably be expected to receive actual notice.” 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

70. Upon information and belief, Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers’ PII and storing and/or sharing that PII on its network.

71. Defendant failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers’ PII on its inadequately secured network and would do so after the customer relationship ended.

72. The Safeguards Rule, which implements Section 501(b) of the GLBA,¹⁵ U.S.C. § 6801(b), requires institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably

foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Defendant violated the Safeguard Rule.

73. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of PII in its custody or control.

74. Defendant failed to design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

75. Defendant failed to adequately oversee service providers.

76. Defendant failed to evaluate and adjust its information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

Defendant Violated the FTC Act

77. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC

publications and orders described above also form part of the basis of Defendant's duty in this regard.

78. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Nationwide Class.

Plaintiff Lin's Experience

79. Plaintiff was required to provide and did provide her PII to Defendant during her use of Defendant's marketplace.

80. To date, Defendant has done next to nothing to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach particularly given the fact that Plaintiff's PII has already been made freely available to anyone wishing to download it.

81. Defendant's data breach notice letter downplays the theft of Plaintiff's and Class Members PII, when the facts demonstrate that the PII was targeted, accessed, and exfiltrated in a criminal cyberattack. Additionally, Plaintiff's and Class members PII is freely available for download to anyone with an internet connection. The fraud and identity monitoring services offered by Defendant are only for two years, and it places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for the service and addressing timely issues when the service number for enrollment does not work properly.

82. Plaintiff and Class Members have been further damaged by the compromise of their PII.

83. Plaintiff's PII was compromised in the Data Breach and was likely stolen and in the hands of cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the PII.

84. Plaintiff typically takes measures to protect her PII and is very careful about sharing her PII. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

85. Plaintiff stores any documents containing her PII in a safe and secure location, and she diligently chooses unique usernames and passwords for her online accounts.

86. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. In response to the Data Breach, Plaintiff has spent significant time monitoring her accounts and credit score and has sustained emotional distress in addition to her lost time. This is time that was lost and unproductive and took away from other activities and duties.

87. Plaintiff suffered multiple identity theft and/or fraud attempts using the information that was compromised during the Data Breach, including attempted loan applications, unknown funds being deposited into her bank account, and others.

88. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

89. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

90. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security Number, being placed in the hands of criminals.

91. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required the PII from Plaintiff when she received services from Defendant. Plaintiff, however, would not have entrusted her PII to Defendant had she known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

92. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

93. Plaintiff brings this suit on behalf of herself and a class of similarly situated individuals under Federal Rule of Civil Procedure 23, which is preliminarily defined as:

All persons Defendant has identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").

94. Plaintiff also seeks to represent a class of Hawaii residents, which is preliminarily defined as:

All persons who are residents of the state of Hawaii and who Defendant has identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Hawaii Subclass").

95. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which

Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

96. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, public news reports indicate that approximately 200,000 individuals had their PII compromised in this Data Breach. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

97. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- i. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;
- ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- iii. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- iv. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- v. Whether Defendant owed a duty to Class Members to safeguard their PII;
- vi. Whether Defendant breached its duty to Class Members to safeguard their PII;

- vii. Whether computer hackers obtained Class Members' PII in the Data Breach;
- viii. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- ix. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- x. Whether Defendant's conduct was negligent;
- xi. Whether Defendant's conduct was *per se* negligent, and;
- xii. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

98. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

99. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

100. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

101. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is

superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

102. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

103. Likewise, particular issues under Federal Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- xiii. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- xiv. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- xv. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- xvi. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

xvii. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

104. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

VI. CAUSES OF ACTION

COUNT I NEGLIGENCE (ON BEHALF OF PLAINTIFF AND THE CLASS)

105. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 104.

106. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

107. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

108. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

109. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's

duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

110. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair. . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

111. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff’s and Class Members’ PII within Defendant’s possession.

112. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff’s and Class Members’ PII.

113. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII within Defendant’s possession might have been compromised and precisely the type of information compromised.

114. Defendant’s breach of duties owed to Plaintiff and Class Members caused Plaintiff’s and Class Members’ PII to be compromised.

115. As a result of Defendant’s ongoing failure to notify Plaintiff and Class Members regarding the type of PII has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

116. Defendant's breaches of duty caused Plaintiff and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their PII.

117. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes.

118. Plaintiff seeks the award of actual damages on behalf of herself and the Class.

119. In failing to secure Plaintiff's and Class Members' PII and promptly notifying them of the Data Breach, Defendant is guilty of oppression, fraud, or malice, in that Defendant acted or failed to act with a willful and conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive damages on behalf of herself and the Class.

120. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to consumer information.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFF AND THE CLASS)

121. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 120.

122. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

123. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

124. Defendant's duty to use reasonable security measures also arose under the GLBA, under which Defendant was required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

125. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

126. Defendant's violation of the GLBA and its Safeguards Rule constitutes negligence *per se*.

127. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes), and the GLBA, were intended to protect.

128. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members. The GLBA, with its Safeguards Rule, was similarly intended.

129. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual

identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT III
VIOLATION OF NORTH CAROLINA UNFAIR TRADE PRACTICES ACT
(ON BEHALF OF PLAINTIFF AND THE CLASS)

130. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 129.

131. Defendant advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

132. Defendant engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures

following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq., which was a direct and proximate cause of the Data Breach;
- d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's Class members' PII; and
- e. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq.

133. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

134. Defendant intended to mislead Plaintiff and Class members and induce them to rely on its omissions.

135. Had Defendant disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the PII that Plaintiff and Class members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff

and Class members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

136. Defendant acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff's and Class members' rights.

137. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

138. Defendant's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

139. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

COUNT IV
HAWAII UNFAIR PRACTICES AND UNFAIR COMPETITION ACT
(ON BEHALF OF PLAINTIFF AND THE HAWAII SUBCLASS)

140. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 139.

141. Plaintiff and Hawaii Subclass members are "consumers" as defined by Haw. Rev. Stat. § 480-1.

142. Plaintiff, the Hawaii Subclass members, and Defendant are “persons” as defined by Haw. Rev. Stat. § 480-1.

143. Defendant advertised, offered, or sold goods or services in Hawaii and engaged in trade or commerce directly or indirectly affecting the people of Hawaii.

144. Defendant engaged in unfair or deceptive acts or practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods and services purchased by Hawaii Subclass members in violation of Haw. Rev. Stat. § 480-2(a), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff’s and Hawaii Subclass members’ PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff’s and Hawaii Subclass members’ PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq., which was a direct and proximate cause of the Data Breach;
- d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff’s Hawaii Subclass members’ PII; and

- e. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq.

145. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

146. Defendant intended to mislead Plaintiff and Hawaii Subclass members and induce them to rely on its omissions.

147. The foregoing unlawful and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous.

148. Defendant acted intentionally, knowingly, and maliciously to violate Hawaii's Unfair Practices and Unfair Competition Act, and recklessly disregarded Plaintiff and Hawaii Subclass members' rights. Defendant's past data breach put it on notice that its security and privacy protections were inadequate.

149. As a direct and proximate result of Defendant's deceptive acts and practices, Plaintiff and Hawaii Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

150. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including actual damages, benefit of the bargain damages, treble damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT V
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE CLASS)

151. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 104.

152. Defendant benefited from receiving Plaintiff's and Class Members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

153. Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

154. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of purchasing services from Defendant, and in connection thereto, by providing their PII to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendant with their PII. In exchange, Plaintiff and Class members should have received adequate protection and data security for such PII held by Defendant.

155. Defendant knew Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

156. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

157. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

158. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

159. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

160. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, request judgment against Defendant and that the Court grant the following:

- A. For an order certifying the Class and Subclass, as defined herein, and appointing Plaintiff and her Counsel to represent each such Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

- i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
- ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
- iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
- v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

- ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- x. requiring Defendant to conduct regular database scanning and securing checks;
- xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and

assess whether monitoring tools are appropriately configured, tested, and updated;

- xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;
- xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

- D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

VIII. JURY TRIAL DEMAND

Plaintiff hereby demands that this matter be tried before a jury.

DATED: August 9, 2022

Respectfully submitted,

s/ Scott Harris

Scott Harris

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

900 W. Morgan Street

Raleigh, North Carolina 27603

Tel.: 919-600-5003

Fax: 919-600-5035

sharris@milberg.com

Gary M. Klinger

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

227 W. Monroe Street, Suite 2100

Chicago, Illinois 60606

Tel.: (866) 252-0878

gklinger@milberg.com